MODIFIKASI METODE KRIPTOGRAFI CAESAR CIPHER MENGGUNAKAN DERET SIMBOL PADA *KEYBOARD SMARTPHONE*

Dwiki Cahyo Yudiantoro

Program Studi Magisteri Teknik Informatika, Universitas Amikom Yogyakarta
Jl. Ringroad Utara, Condongcatur, Sleman, Yogyakarta
dwiki.1121@students.amikom.ac.id

Abstract – Cryptography is widely used as a way for secrets to be conveyed to someone safely. The message is encrypted so that strangers who do not have the right or permission to read the message will not be able to read it. However, the use of cryptography can often be solved by others because the fabricated key of the message is not difficult to solve. In this paper, the author will modify the Caesar Cipher method which produces ciphertext in the form of symbols from a row of keyboards on smartphones and patterns that pass through several methods so that messages are safer and difficult to decrypt. This modified method is expected to enhance security in communication.
Keywords - Cryptography, Caesar Cipher, Ciphertext, Encryption, Decryption

Abstrak - Kriptografi banyak digunakan sebagai cara agar pesan rahasia dapat tersampaikan ke seseorang dengan aman. Pesan tersebut di enkripsi agar orang asing yang tidak memiliki hak atau izin untuk membaca pesan tersebut tidak akan dapat membacanya. Namun, penggunaan kriptografi sering kali dapat dipecahkan atau diselesaikan oleh orang lain karena terkadang kunci dari pesan tersebut tidak sulit untuk dipecahkan. Dalam tulisan ini, penulis akan memodifikasi metode Caesar Cipher yang menghasilkan ciphertext berupa simbol dari deretan keyboard pada smartphone dan pola yang melewati beberapa metode agar pesan lebih aman dan sulit terdekripsi. Metode yang sudah dimodifikasi ini diharapkan dapat mempertinggi keamanan dalam berkomunikasi.
Kata Kunci - Kriptografi, Caesar Cipher, Ciphertext, Enkripsi, Dekripsi

I. PENDAHULUAN

Media komunikasi dijaman sekarang merupakan tindak dari perkembangan teknologi dimana teknologi memang semakin canggih. Ada beberapa cara dalam menjaga kemanan data atau informasi, salah satunya adalah kriptografi yang ada pada saat ini. Pada penerapan kriptografi, tidak hanya melakukan satu teknik saja, tetapi dapat dilakukan dengan cara menggabungkan beberapa metode untuk mengamanan data informasi tersebut. Dengan demikian, dibutuhkan kriptografi dalam mengamankan suatu pesan yang bersifat penting atau pribadi dengan melakukan enkripsi sebelum dikirim ke tujuan, sehingga tingkat keamanan informasi dari pesan tersebut dapat dijamin

Terdapat banyak teknik cara yang dikenal untuk melakukan pengamanan data dan pesan, contoh yang paling dikenal adalah kriptografi yaitu menggunakan teknik penyamaran data dan juga steganografi yang disebut dengan teknik penyembunyian data. Pada penelitian ini penulis hanya menggunakan kriptografi dan memodifikasi metode *Caesar Cipher* yang menghasilkan *ciphertext* berupa simbol dari deretan *keyboard* pada *smartphone* dan pola yang melewati beberapa metode agar pesan lebih sulit terdekripsi. Penelitian ini juga dilakukan agar semakin banyak metode yang dapat dilakukan dalam penerapan kode modifikasi *Caesar Cipher*.

Pada penelitian yang dilakukan oleh Benni Purnama yaitu *A New Modified Caesar Cipher Cryptography Method With Legible Ciphertext from a Message to be Encrypted* [1], penulis memodifikasi *Caesar Cipher* dengan mengganti alfabet menjadi 2 bagian diantaranya mengubah alfabet huruf vokal diganti dengan alfabet vokal juga, dan alfabet konsonan diganti dengan alfabet huruf konsonan. Lalu, huruf tersebut di ubah lagi dengan menggunakan rumus mod 26. Bedanya dengan penelitian yang dilakukan penulis yaitu penulis mengubah huruf alfabet yang ada dengan deret simbol yang ada pada keyboard *smartphone* ASUS dan IPhone. Setelah itu hasil akan di acak kembali dengan deret baris dan zigzag agar hasil enkripsi lebih teracak dan sulit untuk dibaca oleh orang lain.

A. Kriptografi

Kriptografi merupakan ilmu merancang suatu metode untuk memungkinkan seseorang mengirimkan informasi dalam bentuk yang aman dan yang dapat mengambil informasi ini adalah penerima yang dituju[2]. Kriptografi awalnya dilakukan dengan cara manual dengan kerangka yang kurang lebih sama dan dengan banyak perbaikan pada saat implementasi-nya[3].

Kriptografi telah ada lebih dari 2000 tahun yang lalu[4]. Nama *cryptology* adalah gabungan dari kata *cryptos* Yunani (= disembunyikan) dan logo (=studi, sains).oleh karena itu, kata kriptografi secara harfiah berarti ilmu menyembunyikan[5].

Kriptografi disebut juga salah satu ilmu untuk menjaga pengiriman data dengan cara mengubah data yang ingin disampaikan menjadi suatu kode tertentu

serta hanya ditujukan kepada oknum yang berhak dan memiliki kunci rahasia agar dapat mengubah kode itu kembali ke pesan yang seharusnya tersampaikan. Hal ini berfungsi untuk menjaga kerahasiaan suatu pesan maupun data. Dalam kriptografi, data ataupun pesan yang dikirimkan dengan menggunakan jaringan dapat disamarkan. Sehingga apabila data tersebut dapat didapatkan, dipecahkan, dan dibaca oleh oknum lain, maka oknum yang tidak berhak atau tidak memiliki izin untuk mengetahui pesan tersebut tidak akan bisa mengetahui maksud dari data atau pesan yang dikirimkan[6].

Dibidang kriptografi, ada dua konsep terpenting yang disebut juga enkripsi dan dekripsi. Enkripsi merupakan proses suatu informasi atau pesan yang ingin dikirim akan diubah ke dalam bentuk yang hampir tidak dapat dikenali dengan menggunakan metode algoritma tertentu. Dekripsi merupakan lawan dari enkripsi, yaitu mengembalikan bentuk pesan tersembunyi tersebut menjadi pesan awal yang ingin di sampaikan. Sebuah pesan atau data yang masih asli dan belum mengalami proses penyamaran disebut dengan kata *plaintext*. Kemudian setelah dilakukannya penyamaran dengan beberapa cara penyandian, maka *plaintext* itu disebut sebagai *ciphertext*. Dengan kata lain, proses penyamaran dari *plaintext* menjadi *ciphertext* disebut dengan istilah enkripsi (*encryption*), sedangkan proses mengubah kembali dari *ciphertext* ke *plaintext* disebut juga dengan istilah dekripsi (*decryption*)[6].

B. Caesar Cipher Monoalphabetic

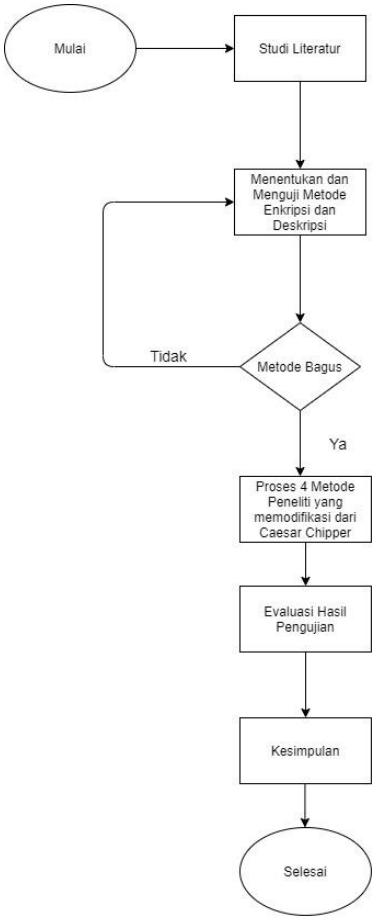
Caesar Cipher merupakan salah satu metode algoritma enkripsi dan dekripsi yang sangat dikenal dan banyak digunakan. Julius Caesar menggunakan cipher aditif untuk berkomunikasi dengan perwiranya. Sehingga cipher aditif ini disebut juga *Caesar Cipher*. Caesar menggunakan 3 kunci untuk berkomunikasi[7]. *Caesar Cipher* adalah jenis cipher subtitusi dimana setiap huruf dalam *plaintext* diganti dengan huruf tetap dibawah alfabet. Misalnya, dengan menggeser 2 huruf yang ada yaitu huruf D menjadi G, E menjadi H, F menjadi I, hingga seterusnya [8].

C. Frekuensi Alfabet pada Text Bahasa Indonesia

Pada komunikasi menggunakan teks. Penggunaan alfabet pada teks dalam Bahasa Indonesia sangat berbeda dengan teks Bahasa Inggris. Dalam Bahasa Inggris, frekuensi kemunculan alfabet tertinggi adalah huruf E[9]. Sedangkan pada Bahasa Indonesia, frekuensi tertinggi adalah huruf A[10]. Dalam kriptografi, ini dilakukan untuk menganalisis berapa kali kunci muncul dalam suatu *ciphertext*.

II. METODE PENELITIAN

Penelitian yang dilakukan oleh penulis merupakan penelitian yang bersifat studi literatur. Metode penelitian yang digunakan dapat dilihat pada Gambar 1.



Gambar 1. Alur Penelitian

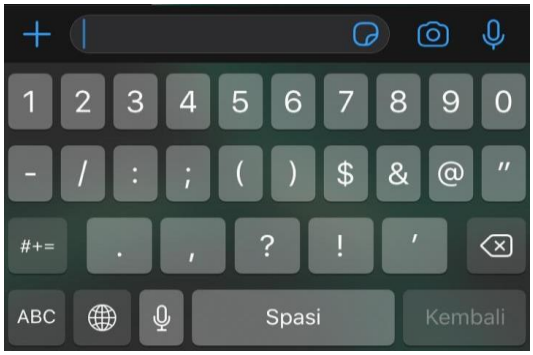
Tahap pertama penulis akan melakukan studi literatur dalam penggunaan *Caesar Cipher*. Lalu penulis akan membuat suatu metode dengan memodifikasi metode *Caesar Cipher* tersebut serta mengujinya, dan didapatkan hasil modifikasi yang menggunakan 4 metode. Lalu penulis melakukan penyembunyian pesan dengan metode tersebut dan melakukan evaluasi sebelum dapat menyimpulkan dan menyelesaikan penelitian ini.

III. HASIL DAN PEMBAHASAN

A. Aturan baru dalam sandi Caesar Penulis

Dalam modifikasi *Caesar Cipher* ini, penulis menggunakan beberapa metode yaitu:

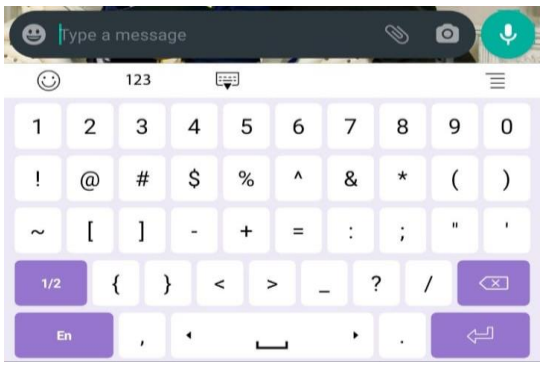
a. Menggunakan 3 kunci yaitu:
   K1= tab pertama pada simbol di *keyboard default* IPhone dengan urutan zigzag yang dimulai dari kiri atas (pada huruf Z, menggunakan simbol pertama cabang dari ' ada pada gambar 5).



Gambar 2. Tab pertama pada simbol di *keyboard default* Iphone

Tambahan simbol di K1 pada huruf alfabet Z menggunakan simbol cabang dikarenakan keterbatasan simbol yang terdapat pada tab *keyboard smartphone* IPhone yang hanya berjumlah 25 simbol.

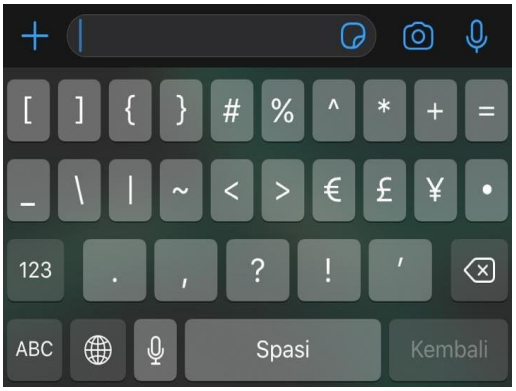
K2=tab pertama pada symbol di *keyboard default smartphone* ASUS dengan urutan zigzag yang dimulai dari baris ke dua kiri.



Gambar 3. Tab pertama pada simbol di *keyboard default smartphone* ASUS

Pada kunci ini, penulis tidak menambahkan simbol tambahan karena simbol pada keyboard *smartphone* ASUS terdapat lebih dari 26 simbol.

K3= tab kedua pada simbol di *keyboard* default IPhone dengan urutan zigzag yang dimulai dari atas kanan (pada huruf Z, menggunakan simbol pertama cabang dari ' ada pada gambar 5).
Pada kunci K3 ini juga sama, tambahan simbol pada huruf Z menggunakan simbol cabang dikarenakan keterbatasan simbol yang terdapat pada tab *keyboard smartphone* IPhone hanya berjumlah 25 simbol.



Gambar 4. Tab kedua pada simbol di *keyboard default* IPhone

Gambar 5. Simbol pertama cabang dari '

b. Pada metode 1, setiap karakter di enkripsi dengan kunci yang berbeda.
c. Pada metode 2, hasil *ciphertext* dirubah menjadi perbaris (3 karakter perbaris).
d. Pada metode 3, baris tersebut kita susun menjadi zigzag.
e. Pada metode 4, ulangi metode 2 dari hasil metode 3.

Hasil akhir di putar dan diurut dari pojok kanan bawah.

B. Menguji Caesar Cipher yang Dimodifikasi
a. Proses Enkripsi
Penulis mencoba membuat susunan kunci sebagai berikut:

Tabel 1. Kunci yang Digunakan

K1	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 1 2 3 4 5 6 7 8 9 0 " @ & $) (; : / - . , ? ! ' `
K2	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z ! @ # $ % ^ & * ( ) ' " ; : = + -] [~ { } < > _ ?
K3	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z = + * ^ % # } {] [_ \ | ~ < > € £ ¥ • ' ! ? , . `

Ketiga kunci ini akan membuat pesan yang disampaikan menjadi tak terbaca dan menjadi susunan simbol yang akan digunakan pada metode berikutnya.

Selanjutnya pada metode 1, penulis mencoba dengan *plaintext* "Selamat menunaikan ibadah puasa" dengan kombinasi kunci K1, K2, dan K3 secara terus menerus. Agar lebih jelas, pada metode 1 didapatkan hasil sebagai berikut:

Tabel 2. Hasil Metode 1

metode 1 setiap karakter di enkripsi dengan kunci yang berbeda																								
Kunci	K1	K2	K3	K1	K2	K3	K1	K2	K3	K1	K2	K3	K1	K2	K3	K1	K2	K3	K1	K2	K3	K1	K2	K3
Plaintext	S	E	L	A	M	A	T	M	E	N	U	N	A	I	K	A	N	I	B	A	D	A	H	P	U	A	S	A
Hasil	/	%	\	=	;	1	-	;	%	~	{	$	1	(	_	=	:	9	2	!	^	=	*	(	.	!	¥	=

Sekarang, *plaintext* yang ada sudah menjadi deretan simbol yang tidak beraturan.

Lalu pada metode ke 2, hasil dari metode 1 diubah perbaris dan apabila baris kurang dari 3 karakter, kita dapat menambahkan simbol "X" pada baris yang ada. Agar lebih jelas, pada metode 2 hasilnya didapat sebagai berikut:

Tabel 3. Hasil Metode 2

/	%	\	1
=	;	1	2
-	;	%	3
~	{	$	4
1	(	_	5
=	:	9	6
2	!	^	7
=	*	(	8
.	!	¥	9
=	X	X	10

Lalu selanjutnya pada metode ke 3, baris tersebut kita susun menjadi zigzag (dimulai dari balok terakhir dan lihat warna agar lebih jelas). Untuk memenuhi zigzag, tambahkan huruf A,B,C,D,E,F,dan seterusnya sehingga didapatkan hasil sebagai berikut:

Tabel 4. Zigzag Metode 3

=	X	X	1	(	_	~	{	$	D	E	F
		.	9					-	C		
	!			:			;			B	
¥					=	%					A
=	*	(	2	!	^	=	;	1	/	%	\

Setelah zigzag terpenuhi, hasil dari metode ini di dapatkan dari menyusun baris atas ke bawah dan di dapatkan hasil sebagai berikut:

Tabel 5. Hasil dari zigzag Metode 3

Hasil dr atas kebawah	=	¥	=	X	!	*	X	.	(	1	9	2	(	:	!	_	=	^	~	%	=	{	;	;	$	-	1	D	C	/	E	B	%	F	A	\

Lalu pada metode 4, kita mengulangi metode ke 2 dari hasil metode ke 3 yaitu menyusun hasil pada metode ke 4 tersebut menjadi zigzag (dimulai dari balok terakhir dan lihat warna agar lebih jelas). Untuk memenuhi zigzag, tambahkan huruf A,B,C,D,E,F,dan seterusnya sehingga didapatkan hasil sebagai berikut:

Tabel 6. Susunan dari Metode 4

=	¥	=	1
X	!	*	2
X	.	(	3
1	9	2	4
(	:	!	5
_	=	^	6
~	%	=	7
{	;	;	8
$	-	1	9
D	C	/	10
E	B	%	11
F	A	\	12

Lalu hasil dari metode ke 4 diurutkan dari pojok kanan bawah dan diurutkan dari kanan ke kiri lalu kiri ke kanan(perhatikan warna agar lebih jelas) sehingga didapatkan hasil sebagai berikut:

Tabel 7. Hasil dari Metode 4

Hasil akhir diurut dari pojok kanan bawah	\	A	F	E	D	$	{	~	_	(	1	X	X	=	¥	!	.	9	:	=	%	;	-	C	B	%	/	1	;	=	^	!	2	(	*	=

Didapatkan hasil akhir yaitu: **\AFED${~_(1XX=¥!.9:=%;-CB%/1;=^!2(*=** sehingga *plaintext* tidak dapat terbaca lagi oleh orang yang tidak berwenang.

b. Proses Dekripsi

Untuk proses dekripsi disini caranya adalah hanya membalik semua metode yang ada dari proses metode 4 hingga kembali ke awal. Proses harus benar-benar mengikuti alur dari akhir metode hingga awal metode dan mengetahui kunci yang dipakai. Oleh karena itu, metode yang digunakan penulis disini terlihat tidak gampang untuk dipecahkan apabila tidak memiliki ketiga kunci dan mengetahui alur metode yang ada.

IV. KESIMPULAN

Dapat dilihat bahwa hasil yang didapatkan adalah berupa symbol yang sudah acak melalui beberapa proses, sehingga cara untuk mendekripsikannya tidak simple. Disini juga terdapat beberapa huruf pelengkap yang membuat enkripsi ini semakin membingungkan pembaca yang tidak mengetahui kunci dari pesan tersebut. Namun, pada penelitian ini, *cipertext* yang dibuat hanya dapat mengubah *plaintext* huruf dan belum bisa mengubah *plaintext* yang berupa angka dan sibmol.

Sebagai saran, penulis selanjutnya dapat menambahkan karakter tertentu agar simbol-simbol yang ada semakin sulit untuk ditebak dan dapat

menambahkan karakter untuk mengubah *plaintext* yang berupa angka dan simbol. Peneliti selanjutnya juga dapat menggunakan steganografi agar pesan enkripsi tidak terlalu terlihat bahwa itu adalah sebuah pesan rahasia.

DAFTAR PUSTAKA

[1] B. Purnama and A. H. H. Rohayani, "A New Modified Caesar Cipher Cryptography Method with LegibleCiphertext from a Message to Be Encrypted," *Procedia Comput. Sci.*, vol. 59, no. Iccsci, pp. 195–204, 2015.

[2] R. Bose, *Information Theory, Coding And Cryptography. Second Edition*. New Delhi: Mc Graw Hill, 2008.

[3] A. Kahate, *Cryptography and Network Security*. New Dehli: Tata McGraw Hill Education Private Limited, 2008.

[4] G. Khasis, Kinger, and Supriya, "Modified Caesar Cipherfor Better Security Enhancement," *Int. J. Comput. Apli cations*, vol. Volume 73, 2013.

[5] J. C. Van Der Lubbe, *Basic Methods Of Cryptography*. United Kingdom: Cambridge University Press, 2002.

[6] F. N. Pabokory, I. F. Astuti, and A. H. Kridalaksana, "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard," *Inform. Mulawarman J. Ilm. Ilmu Komput.*, vol. 10, no. 1, p. 20, 2016.

[7] B. A.Forouzan, *Cryptography and Network Security*. New York: Mc Graw Hill, 2008.

[8] S. B. Dar, "Enhancing The Security of Caesar Cipher Using Double Substitution Method," *Int. J. Comput. Sci. Eng. Technol. ISSN 2229-3345*, vol. Vol.05 No., 2014.

[9] G. Shrivastava, "Using Letters Frequency Analysis in Caesar Cipher with Double Columnar Transposition Technique," *Int. J. Eng. Sci. Res. Technol.*, vol. Vol. 2 Iss, 2013.

[10] A. Hamzah, "Deteksi Bahasa Untuk Dokumen Teks Berbahasa Indonesia," *Semin. Nas. Inform. 2010 (semnasIF 2010) ISSN 1979-2328 UPN "Veteran" Yogyakarta*, 2010.